What is claimed is

1. A method of securely transmitting information comprising the steps of

(a) providing information to be transmitted,

(b) obtaining a fingerprint of a person associated with transmitting the information which fingerprint has ridge endings and bifurcations,

(c) identifying a configuration comprising positions in a planar system of coordinates superimposed onto the fingerprint of a plurality of the ridge endings and bifurcations,

(d) defining an encoding key to encrypt the information which encoding key comprises information derived from the configuration, and

(e) transmitting the encrypted information.

2. The method of claim 1 which further comprises using the encoding key comprising information derived from the configuration as a decoding key to decrypt the encrypted information.

3. The method of claim 1 in which the configuration comprises the positions of all the ridge endings and bifurcations of the fingerprint.

4. The method of claim 1 in which the information to be transmitted comprises plain text.

5. A method of securely transmitting information comprising the steps of

(a) providing information to be transmitted from a first person to a second person,

(b) obtaining a sender fingerprint of the first person and a receiver fingerprint of the second person, each fingerprint having ridge endings and bifurcations,

(c) identifying a first configuration and a second configuration, each configuration respectively comprising positions of a plurality of the ridge endings and bifurcations in a planar system of coordinates superimposed onto the sender fingerprint and the receiver fingerprint,

(d) the first person using the first configuration to create a first encoding key to encrypt the information thereby forming a first cryptogram,

(e) the first person delivering the first encoding key to a key control system independent of the first person and the second person,

(f) the second person using the second configuration to create a second encoding key,

(g) the second person delivering the second encoding key to the key control system,

(h) the first person transmitting the first cryptogram to the key control system,

(i) the key control system decrypting the first cryptogram using the first encoding key as a decoding key to obtain a copy of the information;

(j) the key control system encrypting the copy using the second encoding key as an encoding key and thereby forming a second cryptogram,

(k) the key control system transmitting the second cryptogram to the second person,

(j) the second person decrypting the second cryptogram using the second encoding key as a decoding key.

6. The method of claim 5 which before transmitting the first cryptogram to the key control system over a first route of transmission comprises the first person authenticating that the first route of transmission is secure from tampering.

7. The method of claim 6 in which the authenticating step comprises returning the first encoding key from the key control system to the first person and comparing the returned first encoding key with the first encoding key which had been delivered to the key control system by the first person.

8. The method of claim 5 which before transmitting the second cryptogram to the second person over a second route of transmission comprises the second person authenticating that the second route of transmission is secure from tampering.

9. The method of claim 8 in which the authenticating step comprises returning the second encoding key from the key control system to the second person and comparing the returned second encoding key with the second encoding key which had been delivered to the key control system by the second person.

10. The method of claim 5 further comprising the step of the key control system storing the first encoding key and the second encoding key in separate digital storage media.

11. The method of claim 10 in which the separate digital storage media include a non-rewritable electrical circuit.